Unit-1 Basics of Networking:

Categories of Networks: Local Area Network, Wide Area Network, Metropolitan Area Network, OSI Reference Model, TCP / IP Model.

==========

What is Network?

- A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications.
- The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

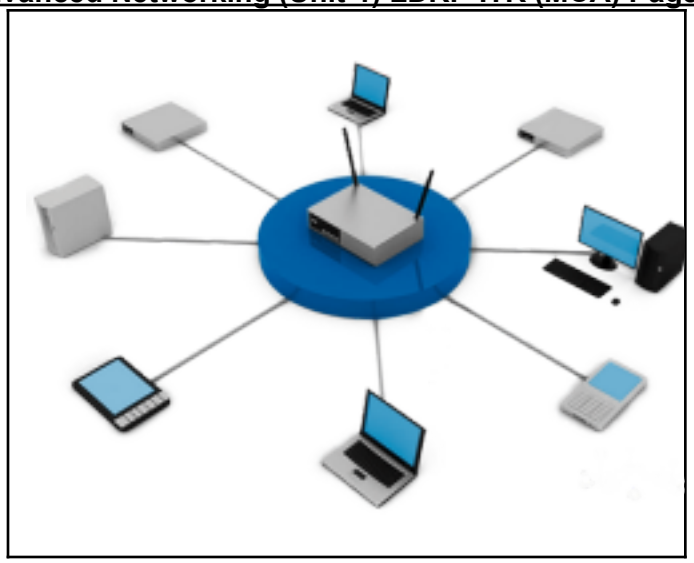
Categories (Types) of Networks.

Depending upon the geographical area covered by a network, it is classified as:

➔ Local Area Network (LAN)
➔ Metropolitan Area Network (MAN)
➔ Wide Area Network (WAN)
➔ Personal Area Network (PAN)

Local Area Network (LAN)

- A LAN is a network that is used for communicating among computer devices, usually within an office building or home.
- LAN's enable the sharing of resources such as files or hardware devices that may be needed by multiple users.
- Is limited in size, typically spanning a few hundred meters, and no more than a mile
- Is fast, with speeds from 10 Mbps to 10 Gbps
- Requires little wiring, typically a single cable connecting to each device
- Has lower cost compared to MANs or WANs
- LAN's can be either wired or wireless. Twisted pair, coax or fiber optic cable can be used in wired LANs.
- LANs are capable of very high transmission rates (100s Mb/s to G b/s). ● Nodes in a LAN are linked together with a certain topology. These topologies include: Bus, Ring and Star



Advantages of LAN:

- ➢ Speed
- ➢ Cost
- ➢ Security
- ➢ Resource Sharing

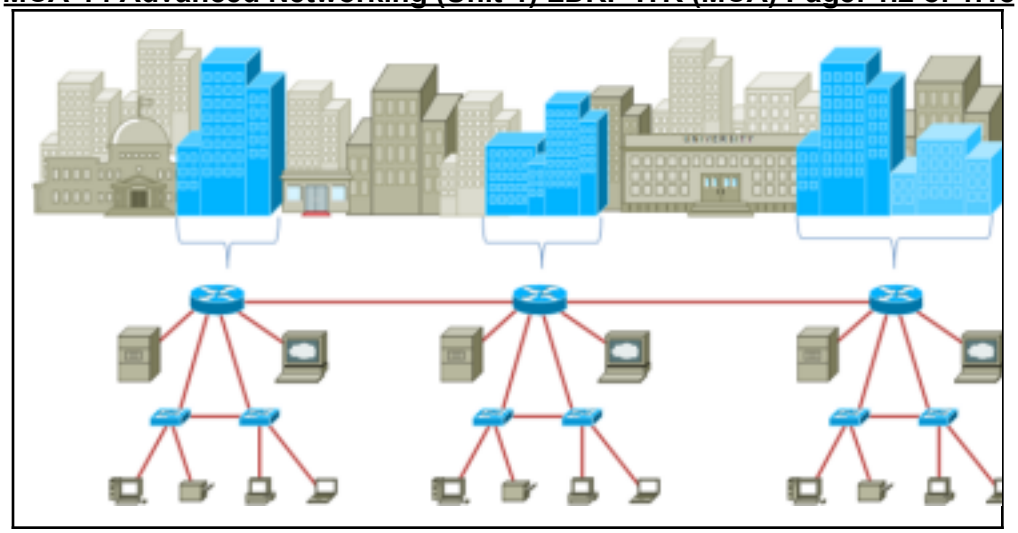
Disadvantages of LAN

- ➢ Expensive To Install
- ➢ Requires Administrative Time
- ➢ File Server May Fail
- ➢ Cables May Break

Metropolitan Area Network (MAN)

- A metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus.
- A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities.
- A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations.
- A MAN often acts as a high speed network to allow sharing of regional resources.

● A MAN typically covers an area of between 5 and 50 km diameter. ● Examples of MAN: Telephone company network that provides a high speed DSL to customers and cable TV network.



MAN

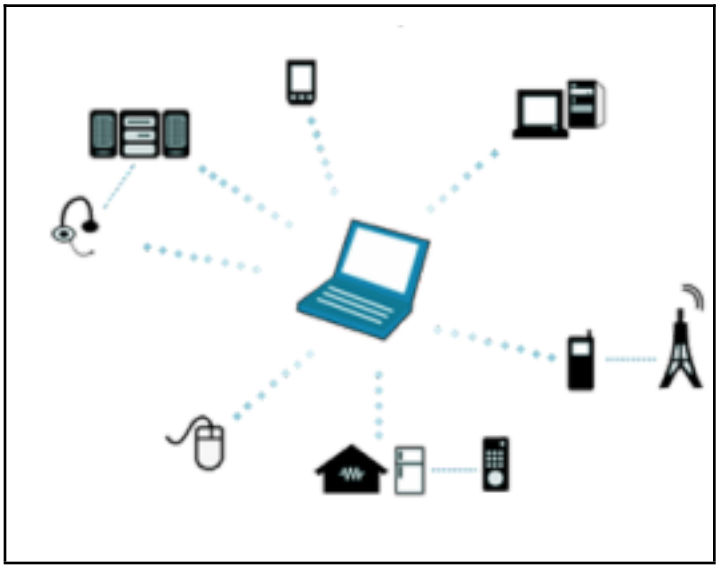
Wide Area Network (WAN)

- WAN covers a large geographic area such as a country, continent or even whole of the world.
- A WAN is two or more LANs connected together. The LANs can be many miles apart.
- To cover great distances, WANs may transmit data over leased high-speed phone lines or wireless links such as satellites.
- Multiple LANs can be connected together using devices such as bridges, routers, or gateways, which enable them to share data.
- The world's most popular WAN is the Internet.

WAN

Personal Area Network (PAN)

- A PAN is a network that is used for communicating among computers and computer devices (including telephones) in close proximity of around a few meters within a room
- It can be used for communicating between the devices themselves, or for connecting to a larger network such as the internet.
- PANs can be wired or wireless.
- A personal area network (PAN) is a computer network used for communication among computer devices, including telephones and personal digital assistants, in proximity to an individual's body.
- The devices may or may not belong to the person in question. The reach of a PAN is typically a few meters.

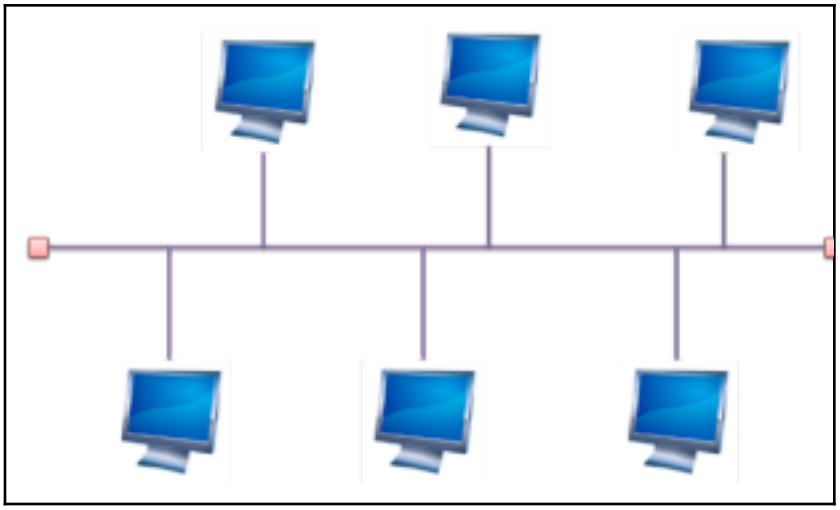


PAN

Network Topologies

- Topology refers to the way in which the network of computers is connected.
- A network topology is the physical and logical arrangement of nodes and connections in a network. Nodes usually include devices such as switches, routers and software with switch and router features. Network topologies are often represented as a graph.
- Each topology is suited to specific tasks and has its own advantages and disadvantages.

Bus Topology:



● In Bus Topology, all stations attach through appropriate hardware interfacing known as a tap, directly to a linear transmission medium, or bus. ● A shared link is used between different stations. Hence it is very cost effective.

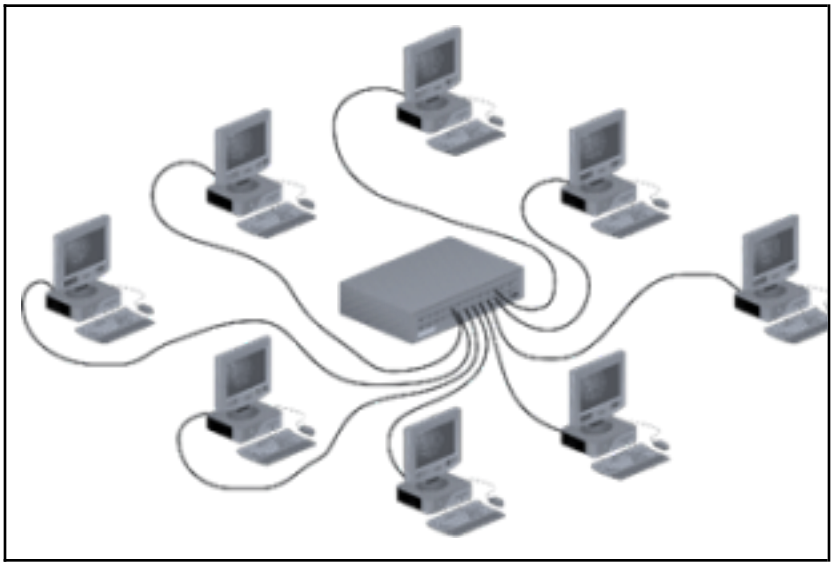
- One can easily add any new node or delete any node without affecting other nodes.
- A transmission from any station propagates the length of the medium in both directions and can be received by all other stations.
- Suitable medium access control technique should be used so as to provide some way to decide “who” will go next to send data?
- If the sender sends data (signal) with a small strength signal, the farthest station will not be able to receive the signal properly.

Advantages	Disadvantages
Cheap and Easy to implement	Network disruption when computers are added or removed
Require less cable	A break in the cable will prevent all systems from accessing the network.
Does not use any specialized network equipment.	Difficult to troubleshoot.

Star Topology:

- In the star topology, each station is directly connected to a common central node.
- Typically, each station attaches to a central node, referred to as the star coupler, via two point-to-point links, one for transmission and one for reception.
- Very High speeds of data transfer can be achieved by using star topology, particularly when the star coupler is used in the switch mode.
- This topology is the easiest to maintain, among the other topologies. ● As

the number of links is proportional to n, this topology is very flexible and is the most preferred topology.

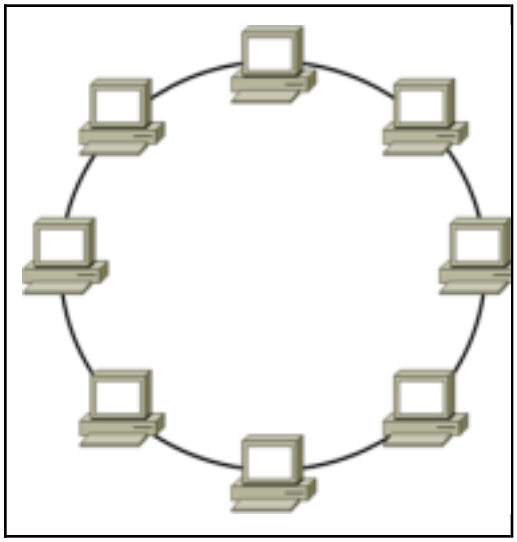


STAR Topology

Advantages	Disadvantages
Easily expanded without disruption to the network	Requires more cable
Cable failure affects only a single user	If the central connecting device fails, the whole network fails.
Easy to troubleshoot and isolate problems	More difficult to implement

Ring Topology:

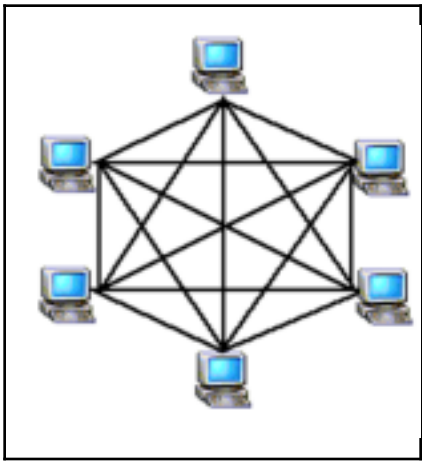
- In the ring topology, the network consists of a set of repeaters joined by point-to-point links in a closed loop.
- The Connector is a comparatively simple device, capable of receiving data on one link and transmitting them, bit by bit, on the other link as fast as they are received, with no buffering.
- The links are unidirectional; that is data are transmitted in one direction only and all are oriented in the same way.



Advantages	Disadvantages
Cable faults are easily located, making troubleshooting easier.	Expansion to the network can cause network disruption.
Ring networks are moderately easy to install.	A single break in the cable can disrupt the entire network.

Mesh Topology:

- In this topology each node or station is connected to every other station ● Two nodes are connected by dedicated point-point links between them. ● So the total number of links to connect n nodes = n(n-1)/2; which is proportional to n2.
- Media used for the connection (links) can be twisted pair, coaxial cable or optical fiber.
- Mesh Topology is not flexible and has a poor expandability as to add a new node n number of links have to be laid.

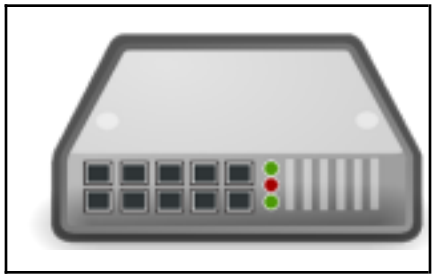


Advantages	Disadvantages
Provides redundant paths between devices.	Requires more cable than the other LAN topologies.
The network can be expanded without disruption to current uses.	Complicated implementation.

Network Devices.

Hub:

- Hubs are simple network devices, and their simplicity is reflected in their low cost.
- Computers connect to a hub via a length of twisted-pair cabling. ● The basic function of a hub is to take data from one of the connected devices and forward it to all the other ports on the hub.
- This method of operation is inefficient because, in most cases, the data is intended for only one of the connected devices.
- Hubs are now largely obsolete, having been replaced by network switches except in very old installations.
- A hub/repeater has no memory to store any data in – a packet must be transmitted while it is received and it is lost when a collision occurs.



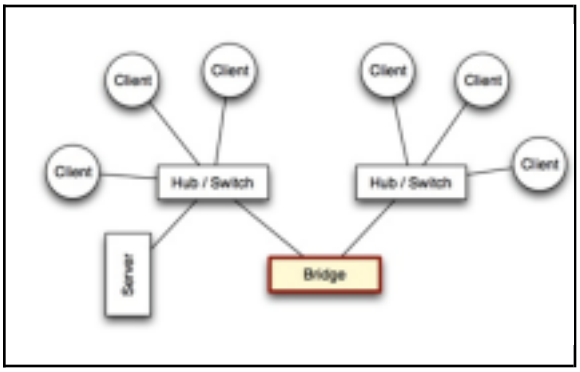
Switch:

- On the surface, a switch looks much like a hub.
- Despite their similar appearance, switches are far more efficient than hubs and are far more desirable for today's network environments. ● Rather than forwarding data to all the connected ports, a switch forwards data only to the port on which the destination system is connected. ● By forwarding data only to the system to which the data is addressed, the switch decreases the amount of traffic on each network link dramatically. ● No collisions means no need to detect collisions—thus, a collision-detection system is not needed with switches.

Bridge:

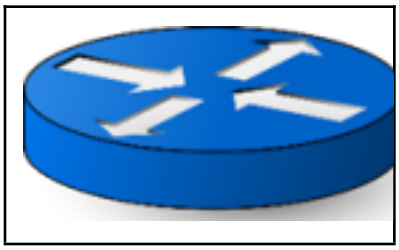
- Bridges are networking devices that connect networks.
- Sometimes it is necessary to divide networks into subnets to reduce the amount of traffic on each larger subnet or for security reasons. ● Today, network switches have largely replaced bridges.
- The basic function of a bridge is blocking or Forwarding.
- If the bridge believes the destination address is on a network other than that from which the data was received, it can forward the data to the other networks to which it is connected.
- If the address is not on the other side of the bridge, the data is blocked from

passing.



Router:

- A router is a networking device that forwards data packets between computer networks.
- By examining data as it arrives, the router determines the best way for the data to continue its journey.
- More commonly, a router is used to provide connectivity across wide area network (WAN) links.
- Routers are an increasingly common sight in any network environment, from a small home office that uses one to connect to an Internet service provider (ISP) to a corporate IT environment where racks of routers manage data communication with disparate remote sites.



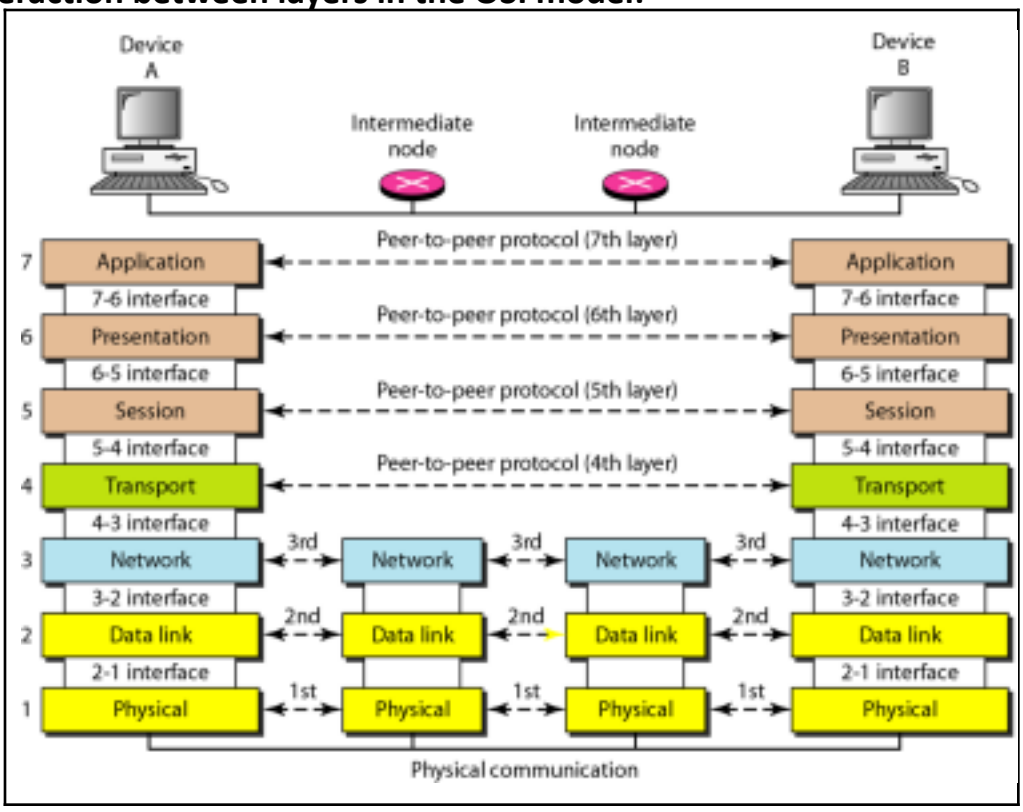
OSI (Open Systems Interconnection) Reference Model:

- It was established in 1947, by ISO. The International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards.
- Here, ISO is an organization and OSI is the model.
- It is divided into seven layers that work together to carry out specialized network functions, allowing for a more systematic approach to networking. ●

The OSI model consists of seven abstraction layers arranged in a top-down order:

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

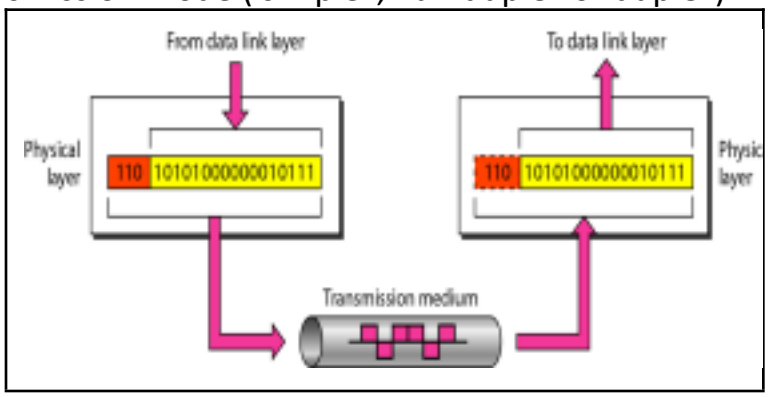
The interaction between layers in the OSI model:



Physical Layer:

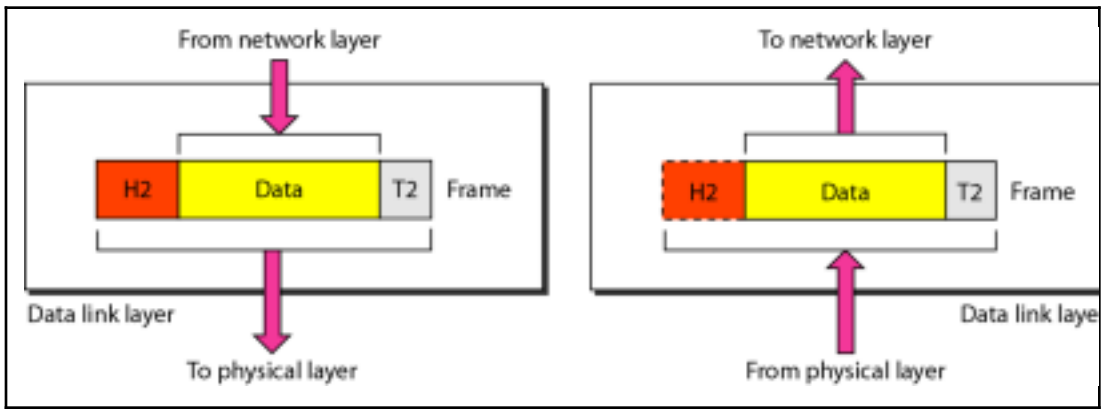
- The physical layer is responsible for movement of individual bits from one hop (node) to the next.
- The physical layer contains information in the form of bits.
- Functions of Physical Layer are,

- Physical characteristics of interfaces and media
- Representation of bits
- Data rate
- Synchronization of bits
- Transmission mode (simplex, half-duplex or duplex)



Data Link Layer:

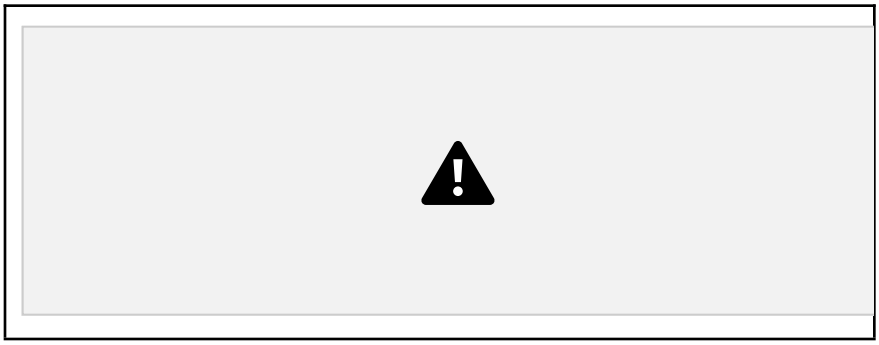
- The Data Link Layer is responsible for moving frames from one hop (node) to the next.
- Packet in the Data Link layer is referred to as Frame.
- Switch & Bridge are Data Link Layer devices.
- When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its Media Access Control (MAC) address. A MAC Address is a 12-digit hexadecimal number which is worldwide unique since millions of network devices exist and we need to uniquely identify each.
- Functions of the Data Link Layer are,
  - Framing
  - Physical addressing (Through MAC address.)
  - Error control
  - Flow Control
  - Access control



Network Layer:

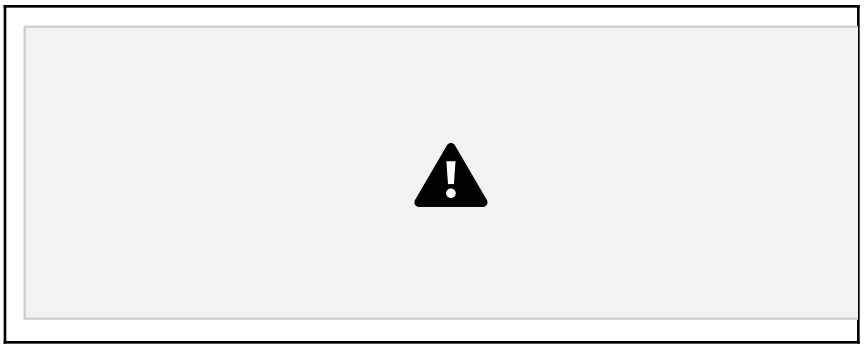
- The network layer is responsible for the delivery of individual packets from the source host to the destination host.
- It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.
- The sender & receiver's IP addresses are placed in the header by the network layer.
- Network layer is implemented by networking devices such as routers and switches.

- Functions of the Network Layer are,
  - Routing: The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
  - Logical Addressing: To identify each device on Internetwork uniquely, the network layer defines an addressing scheme. It uses IP addresses for identification.



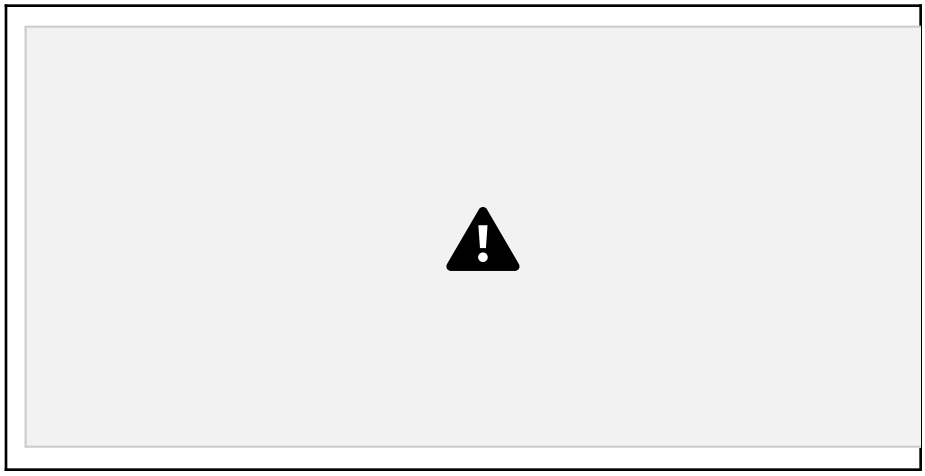
Transport Layer:

- The transport layer is responsible for the delivery of a message from one process to another. (Process to Process delivery)
- The data in the transport layer is referred to as Segments.
- It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.
- Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls. ● Functions of the Transport Layer are,
    - Port addressing
    - Segmentation and Reassembly
    - Connection control (Connection oriented and connection less)
    - Flow Control, Error control



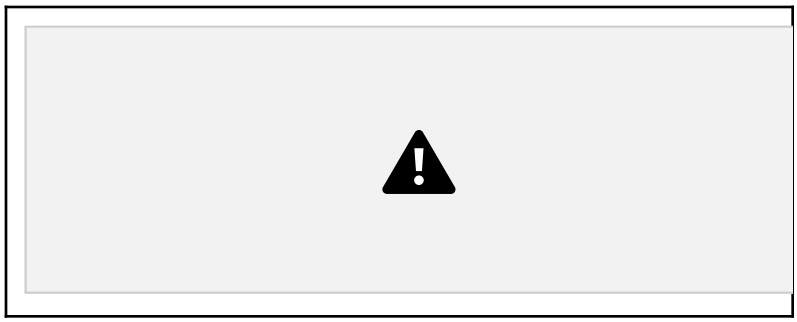
Session Layer:

- The session layer is responsible for dialog control and synchronization. ● It establishes, maintains and synchronizes the interaction between communicating systems.
- Functions of the Session Layer are,
    - Session establishment, maintenance, and termination
    - Synchronization
    - Dialog Controller (half-duplex or full-duplex)



Presentation Layer:

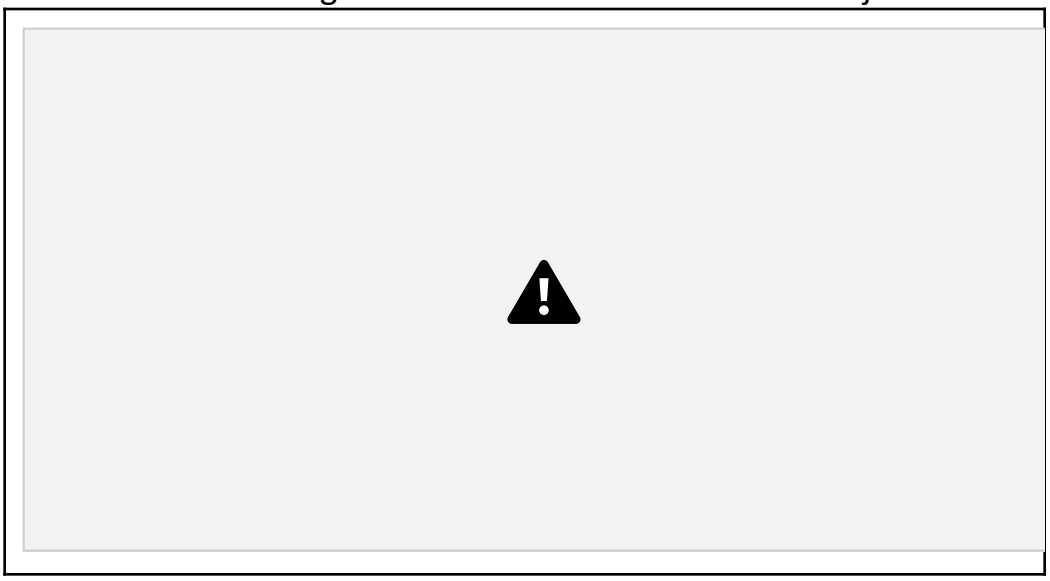
- The presentation layer is responsible for translation, compression, and encryption.
- The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
- Functions of the Presentation Layer are,
    - Translation: For example, ASCII to EBCDIC.
    - Encryption/ Decryption: Data encryption translates the data into unreadable form.
    - Compression: Reduces the number of bits that need to be transmitted on the network.



Application Layer:

- The application layer is responsible for providing services to the user.
- The application Layer is also called Desktop Layer.
- Functions of the Application Layer are,

- Network Virtual Terminal (Remote Login)
- File transfer, access and management
- Mail Services: Provide email service.
- Directory Services: This application provides distributed database sources
- and access for global information about various objects and services.

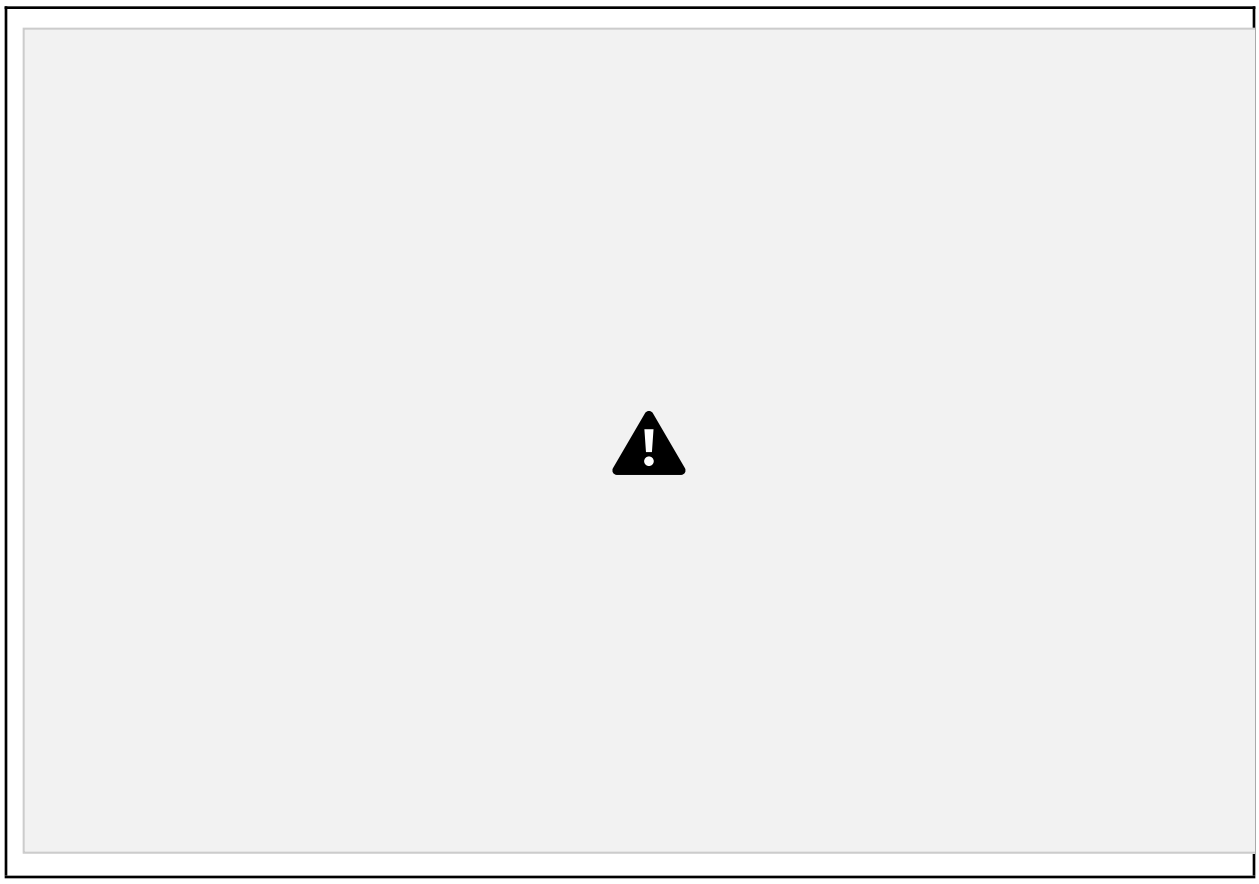


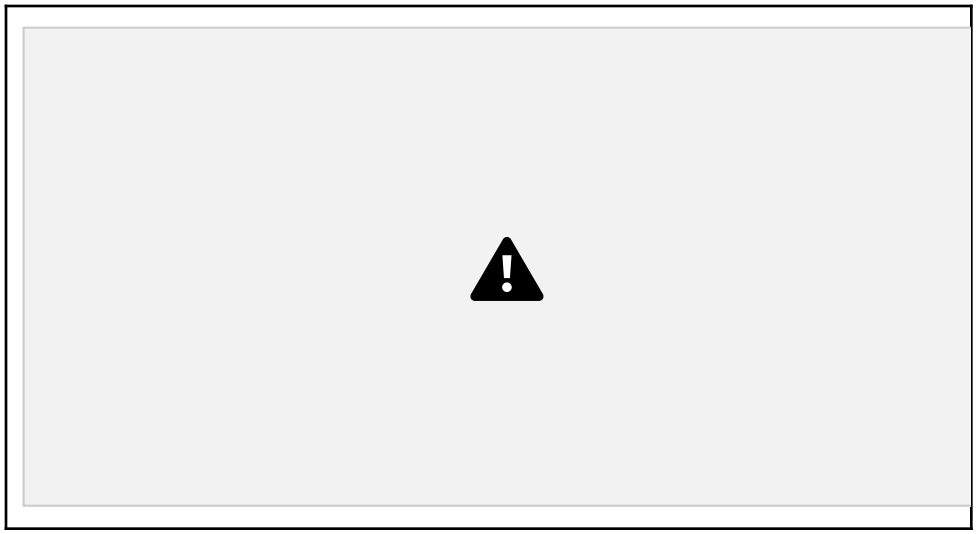
TCP / IP Model:

The OSI Model we just looked at is just a reference/logical model. TCP/IP was designed and developed by the Department of Defense (DoD) in the 1960s and is based on standard protocols.

The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model.

Whenever we want to send something over the internet using the TCP/IP Model, the TCP/IP Model divides the data into packets at the sender's end and the same packets have to be recombined at the receiver's end to recover the same data.





Network Access (Host to Network) Layer:

- This layer is responsible for generating the data and requesting connections.

Network (Internet) Layer:

- It defines the protocols which are responsible for the logical transmission of

data over the entire network. The main protocols residing at this layer are as follows:

- **IP:** IP stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers.
- **ICMP:** ICMP stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
- **IGMP:** The Internet Group Management Protocol (IGMP) is a protocol that allows several devices to share one IP address so they can all receive the same data.
- **ARP:** ARP stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address.
- **RARP:** Reverse Address Resolution Protocol is finding IP addresses from the hardware address.

Transport Layer:

The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error.

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are transport layer protocols at this level.

Basis	**Transmission Control Protocol (TCP)**	**User Datagram Protocol (UDP)**
Type of Service	TCP is a connection-oriented protocol	UDP is the Datagram-oriented connectionless protocol.
Reliability	TCP is reliable and guaranteed.	The delivery of data to the destination cannot be guaranteed in UDP.

Error checking mechanism TCP provides extensive	error-checking mechanisms UDP has only the basic	error-checking mechanism using checksums.

Acknowledgment	An acknowledgment segment is present.	No acknowledgment segment.
Sequence	Sequencing of data is a feature of the Transmission Control Protocol (TCP).	There is no sequencing of data in UDP
Speed	TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.
Retransmission	Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in UDP.
Weight	TCP is heavy-weight.	UDP is lightweight.
Handshaking Techniques	Uses handshakes such as SYN, ACK, SYN-ACK	It's a connectionless protocol i.e. No handshake
Broadcasting	TCP doesn't support Broadcasting.	UDP supports Broadcasting.

Application Layer:

- It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. ● The main protocols present in this layer are:
    - HTTP (Hypertext Transfer Protocol) and HTTPS,
    - FTP (File Transfer Protocol),

- SMTP (Simple Mail Transfer Protocol),
- DNS (Domain Name Systems),
- SNMP (Simple Network Management Protocol),
- TELNET (Teletype network) etc.